NETSCREEN-200 SERIES

User's Guide

Version 5.0 P/N 093-1253-000 Rev. B

Copyright Notice

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Contents

Preface

The Juniper Networks NetScreen-200 Series consists of versatile, purpose-built, high-performance security systems that provide IPSec VPN and firewall services for medium and large enterprise offices, e-business sites, data centers, and carrier infrastructures.

The NetScreen-200 Series includes the following device models:

- The NetScreen-204, which has four 10/100 Base-T interface ports and performs firewall functions at 400 Mbps
- The NetScreen-208, which has eight 10/100 Base-T interface ports and performs firewall functions at 550 Mbps

All NetScreen-200 Series 10/100 Base-T ports perform auto-speed sensing and auto-polarity correction.

GUIDE ORGANIZATION

This manual has three chapters and one appendix.

Chapter 1, "Overview"provides a detailed overview of the system and its components.

Chapter 2, "Installing the Device"describes how to rack-mount the NetScreen-200 systems and connect the systems to other devices.

Chapter 3, "Configuring the Device"details how to connect the NetScreen-200 device to the network and perform initial configuration.

Appendix A, "Specifications" provides a list of physical specifications about the NetScreen-200 Series, the modules, and power supplies.

COMMAND LINE INTERFACE (CLI) CONVENTIONS

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example,

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 }
  manage
  ```

  means "set the management options for the ethernet1, ethernet2, or ethernet3 interface".

- Variables appear in *italic*. For example:

  set admin user *name1* **password** *xyz*

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in *italic*). For example: "Use the **get system** command to display the serial number of a NetScreen device."

Note: *When typing a keyword, you only have to type enough letters to identify the word uniquely. For example, typing* ***set adm u joe j12fmt54*** *is enough to enter the command* ***set admin user joe j12fmt54****. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.*

JUNIPER NETWORKS NETSCREEN PUBLICATIONS

To obtain technical documentation for any Juniper Networks NetScreen product, visit www.juniper.net/techpubs/.

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

techpubs-comments@juniper.net

Overview 1

This chapter provides detailed descriptions of the NetScreen-200 Series system devices and their components.

Topics in this chapter include:

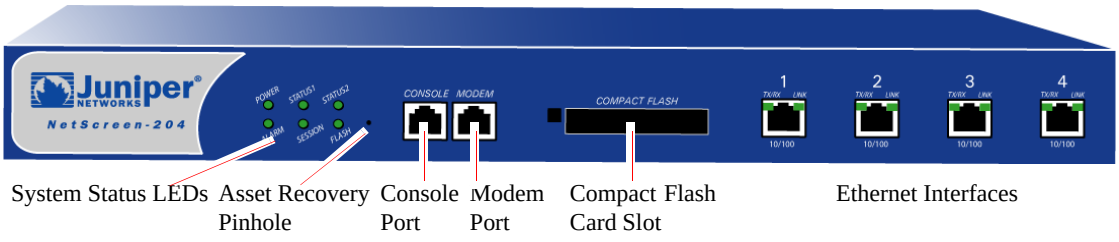
Note: *For safety warnings and instructions, please refer to the* NetScreen Safety Guide. *The instructions in this guide warn you about situations that could cause bodily injury. Before working on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.*

NETSCREEN-200 SYSTEMS

This NetScreen-200 Series currently includes the NetScreen-204 device and the NetScreen-208 device.

NetScreen-204 Device

The NetScreen-204 is a chassis-based, rack-mountable network security device with four ethernet 10/100 Base-T interface ports. The figure below shows a NetScreen-204 device.



System Status LEDs | Asset Recovery Pinhole | Console Port | Modem Port | Compact Flash Card Slot | Ethernet Interfaces

NetScreen-208 Device

The NetScreen-208 is a chassis-based, rack-mountable network security device with eight ethernet 10/100 Base-T interface ports. The figure below shows a NetScreen-208 device.

System Status LEDs | Asset Recovery Pinhole | Console Port | Modem Port | Compact Flash Card Slot | Ethernet Interfaces

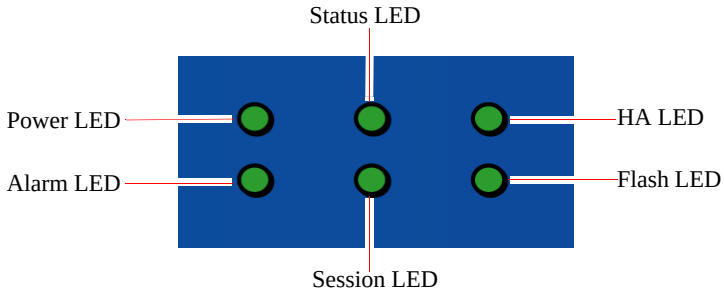
The Front Panel

The features shared in common by NetScreen-204 and NetScreen-208 devices include:

- A System Status LED display
- An Asset Recovery Pinhole
- A Console port
- A Modem port
- A Compact Flash Card Slot
- Ethernet interfaces

System Status LED Display

The front panel of each NetScreen-200 Series device has a System Status display, which contains six LEDs.



The information revealed by each LED is as follows:

LED Name	Purpose	Color	Meaning
Power	Power Supply	**green**	Power supply is functioning correctly.
		off	The device is not receiving power.
Status	System Status	**amber**	At initial power up.
		green	At startup and while performing diagnostics.
		blinking green	Normal operation.
		blinking red	Error detected
HA	High Availability Status	**green**	Unit is the primary (master) device.
		blinking green	Connection not found.
		amber	Unit is the secondary (backup) device.
		off	HA not enabled.

Alarm	System Alarm	**red**	Critical alarm: • Failure of hardware component or software module (such as a cryptographic algorithm). • Firewall attacks detected.
		amber	Major alarm: • Low memory (less than 10% remaining). • High CPU utilization (more than 90% in use). • Session full. • Maximum number of VPN tunnels reached. • HA status changed or redundant group member not found.
		off	No alarms.
Session	Session Utilization	**amber**	Session utilization is between 70% and 90%.
		red	Session utilization is greater than 90%.
		off	Normal operation.
Flash	Memory Card Status	**green**	The card is installed.
		blinking green	Read-write activity is detected.
		off	Flash card slot is empty.

Asset Recovery Pinhole

The Asset Recovery Pinhole is a button that resets the device to its original default settings. To use this button, insert a stiff wire (such as a straightened paper clip) into the pinhole.

Warning: *Because resetting the device restores it to the original default configuration, any new configuration settings are lost, and the firewall and all VPN service become inoperative.*

Console and Modem Ports

The Console port is an RJ-45 serial console port connector, for vt100 terminal emulator programs to perform local configuration and administration.

The Modem port is an RJ-45 serial console port connector, for establishing remote console sessions using dialup connections through a 9600 bps modem connected via an RS-232 cable. Dialing into the modem establishes the dialup console connection.

The table below lists the RJ-45 to DB-9 adapter connection definitions. To employ a standard UART port, both the console and the modem ports use this configuration.

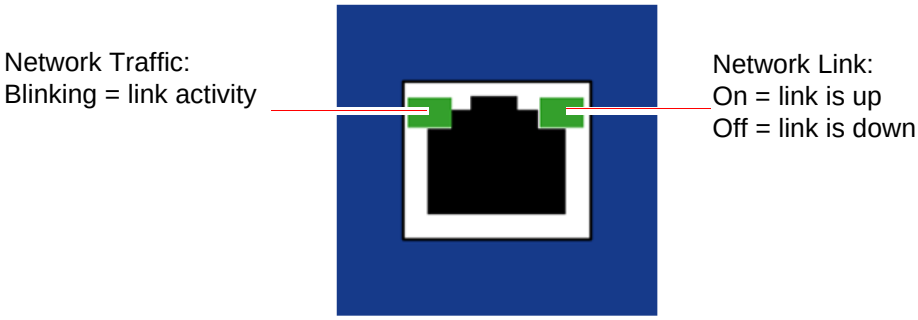
DB9	Signal	Abbreviation	DTE	DCE	RJ-45
1	Data Carrier Detect	DCD	In	Out	NC
2	Received Data	RD	In	Out	3
3	Transmitted Data	TD	Out	In	6
4	Data Terminal Ready	DTR	Out	In	7
5	Signal Ground	SGND	N/A	N/A	4
6	Data Set Ready	DSR	In	Out	2
7	Request To Send	RTS	Out	In	8
8	Clear To Send	CTS	In	Out	1
9	Ring Indicator	RI	In	Out	NC

Compact Flash Card Slot

The NetScreen-200 Series supports CompactFlash™ cards with a variety of memory capacities. NetScreen has tested SanDisk 96MB and 512MB cards. The NetScreen device automatically detects the presence of a flash card and records the system log to it.

Ethernet Interfaces

Each Ethernet port is a 10/100 auto-sensing interface with two link LEDs. The left LED indicates network traffic, and the right LED indicates an active network link.



The Rear Panel

The figure below shows the rear panel of a NetScreen-200 Series device (with an AC power supply).

Note: *Certain export restrictions may apply to international customers. Check with your sales representative.*

Power Supplies

A NetScreen-200 Series device can have an AC power supply or a DC power supply.

The DC power supply can operate on one or two DC feeds ranging from -36V to -60V. When you use two feeds, they share the load. If one feed fails, the other automatically assumes the full load.

The internal fuse for the DC power supply is a 3.15A/250V, fast-acting fuse. This is not replaceable.

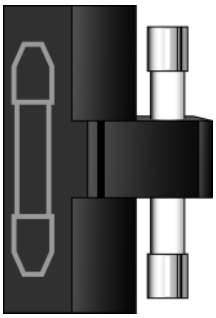
Power Fuse

Each NetScreen-200 Series device uses a 2.5 Amp, slow-blow power fuse rated for 250 Volts.

To replace a fuse on a NetScreen-200 Series device:

1. Take the device off-line by turning the power switch OFF and disconnecting the power cable.
2. Using a screwdriver, separate the lid of the external fuse cover from the surface of the power outlet.

3. Gently remove the fuse assembly.
4. Slide the new fuse into the opening until the fuse clicks into place.



5. Replace the power cable, then turn the device power switch ON.

2

Installing the Device

This chapter describes how to install a device in an equipment rack or on a desktop, and how to connect the device to other devices.

Topics in this chapter include:

Note: *For safety warnings and instructions, please refer to the NetScreen Safety Guide. The instructions in this guide warn you about situations that could cause bodily injury. Before working on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.*

General Installation Guidelines

Observing the following precautions can prevent injuries, equipment failures and shutdowns.

- Never assume that the power supply is disconnected from a power source. *Always* check first.
- Room temperature might not be sufficient to keep equipment at acceptable temperatures without an additional circulation system. Ensure that the room in which you operate the device has adequate air circulation.
- Do not work alone if potentially hazardous conditions exist.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.

Note: *To prevent abuse and intrusion by unauthorized personnel, it is extremely important to install the NetScreen device in a locked-room environment.*

Performing Equipment-Rack Installation

Although you can install a NetScreen-200 Series device on a desktop, it is advisable to install the device in an equipment rack if possible.

Equipment Rack Installation Guidelines

The location of the chassis and the layout of your equipment rack or wiring room are crucial for proper system operation.

Use the following guidelines while configuring your equipment rack.

- Enclosed racks must have adequate ventilation. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or exhaust ports. If you install the chassis on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, equipment higher in the rack can draw heat from the lower devices. Always provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can isolate exhaust air from intake air. The best placement of the baffles depends on the airflow patterns in the rack.

You can mount the device in a standard 19-inch equipment rack. Rack mounting requires the following tools:

- 1 Phillips-head screwdriver
- Rack-compatible screws
- The supplied front-mount brackets
- The supplied mid-mount brackets

There are two ways to rack-mount the NetScreen-200 Series:

- Front mount
- Mid-mount

Front Mount

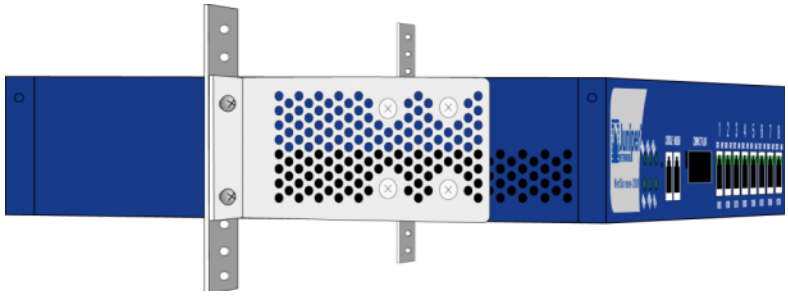
To front mount the NetScreen-200 Series device on your equipment rack:

1. Screw the front mount bracket to the side of the chassis.
2. Screw the front mount bracket to the rack, as shown below.

Mid-Mount

To mid-mount the NetScreen-200 Series device on your equipment rack:

1. Screw the mid-mount bracket to the side of the chassis.
2. Screw the mid-mount bracket to the rack, as shown below.



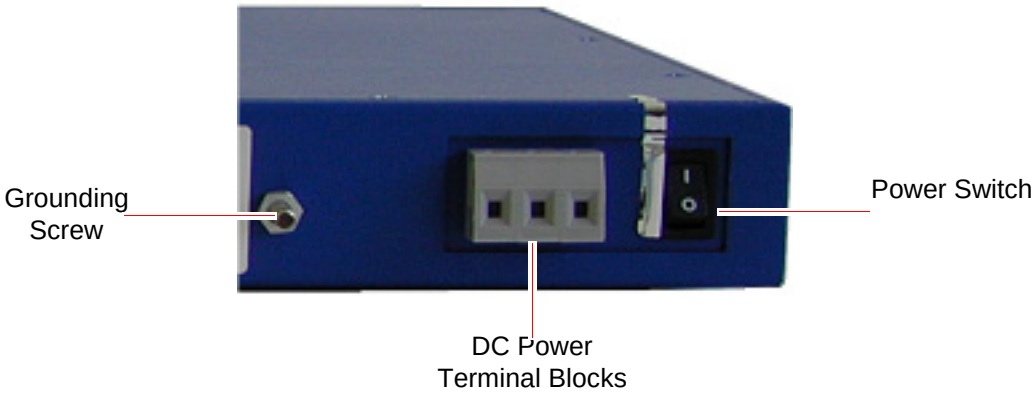
Connecting the Power

To connect the power supply to the NetScreen-200 Series device:

1. Plug the female end of a power cable into the male power receptacles on the back of the system.
2. Turn the Power switch ON.

Wiring a DC Power Supply

The DC power supply, ON/OFF switch, grounding screw, and terminal blocks, are located in the back of the chassis of the power supply unit.



Warning: *You must shut off the current to the DC feed wires before connecting the wires to the power supplies. Also, make sure that the ON/OFF switch is in the OFF position.*

To connect the DC power supply to a grounding point at your site:

1. Remove the hex nut on the grounding screw.
2. Place the ground lug on the screw then tighten the hex nut securely.
3. Connect the other end of the grounding lug wire to a grounding point at your site.

NetScreen-200 Series devices can operate on one or two feeds. To connect DC power feeds to the terminal blocks:

1. Strip the ends of the power cables.
2. Loosen the three screws in the top of the block. (These are captive screws, which you cannot completely remove.)
3. Insert the 48V DC power feed wires into the two outside receptacles of the terminal block.
4. Insert the 0V DC feed wires into the center receptacle.
5. Tighten the screws over the receptacles.

CONNECTING THE NETSCREEN-200 DEVICE TO OTHER DEVICES

To connect the device, use the ethernet interfaces (**ethernet1** through **ethernet4** on the NetScreen-204, or **ethernet1** through **ethernet8** on the NetScreen-208). The purpose of each interface depends upon the security zone to which it is bound.

By default, the zone and interface bindings are as follows:

- **ethernet1** is bound to the Trust security zone by default.

  Connect this interface using a twisted pair cable with RJ-45 connectors.
- **ethernet2** is bound to the DMZ security zone by default.

  Connect this interface using a twisted pair cable with RJ-45 connectors.
- **ethernet3** is bound to the Untrust security zone by default.

  Connect this interface using a twisted pair cable with RJ-45 connectors.
- **ethernet4** through **ethernet8**: Can be connected as required.

The default IP address of each ethernet interface is 0.0.0.0/0.

For information on interfaces and security zones, see "The NetScreen-200 Series Device Interfaces" on page 17.

3

Configuring the Device

This chapter describes how to perform initial configuration on a NetScreen-200 Series device once you have mounted it in a rack or desktop, plugged in the necessary cables, then turn the power ON.

Topics in this chapter include:

Note: *You must register your product at www.juniper.net/support/ so that certain ScreenOS services, such as the Deep Inspection Signature Service, can be activated on the device. After registering your product, use the WebUI or CLI to obtain the subscription for the service. For more information about registering your product and obtaining subscriptions for specific services, see the "System Parameters" chapter in Volume 2 of the* NetScreen Concepts & Examples ScreenOS Reference Guide.

Note: *If you access the device for the first time using the ScreenOS WebUI graphical interface, the Initial Configuration Wizard appears when you log in to the WebUI. This Wizard guides you through the configuration described in this chapter. For more information about starting the Initial Configuration Wizard, refer to the* Juniper Networks NetScreen-200 Series Getting Started Guide.

OPERATIONAL MODES

The NetScreen-200 Series device supports two device modes: Transparent mode and Route mode. The default mode is Route.

Transparent Mode

In Transparent mode, the NetScreen-200 device operates as a Layer-2 bridge. Because the device cannot translate packet IP addresses, it cannot perform Network Address Translation (NAT). Consequently, for the device to access the Internet, any IP address in your trusted (local) networks must be routable and accessible from untrusted (external) networks.

In Transparent mode, the IP addresses for the Layer-2 Trust and Untrust zones are 0.0.0.0, thus making the NetScreen device invisible to the network. However, the device can still perform firewall, VPN, and traffic management according to configured security policies.

Route Mode

In Route mode, the NetScreen-200 device operates at Layer 3. Because you can configure each interface using an IP address and subnet mask, you can configure individual interfaces to perform NAT.

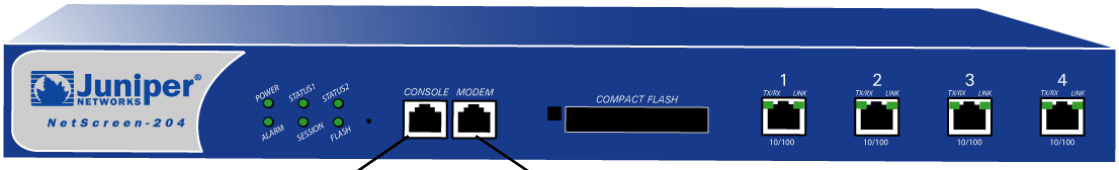
- When the interface performs NAT services, the device translates the source IP address of each outgoing packet into the IP address of the untrusted port. It also replaces the source port number with a randomly-generated value.
- When the interface does *not* perform NAT services, the source IP address and port number in each packet header remain unchanged. Therefore, to reach the Internet your local hosts must have routable IP addresses.

For more information on NAT, see the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Note: *Performing the setup instructions below configures your device in Route mode. To configure your device in Transparent mode, see the* NetScreen Concepts & Examples ScreenOS Reference Guide.

The NetScreen-200 Series Device Interfaces

Each NetScreen-200 device provides ethernet interfaces for access and connectivity. In addition, there are logical (non-physical) interfaces that perform special Layer-2 or management functions.



Console Port Modem Port Ethernet Interfaces **ethernet1** through **ethernet4**

Console Port Modem Port Ethernet Interfaces **ethernet1** through **ethernet8**

The configurable interfaces available on a NetScreen-200 Series device are as follows:

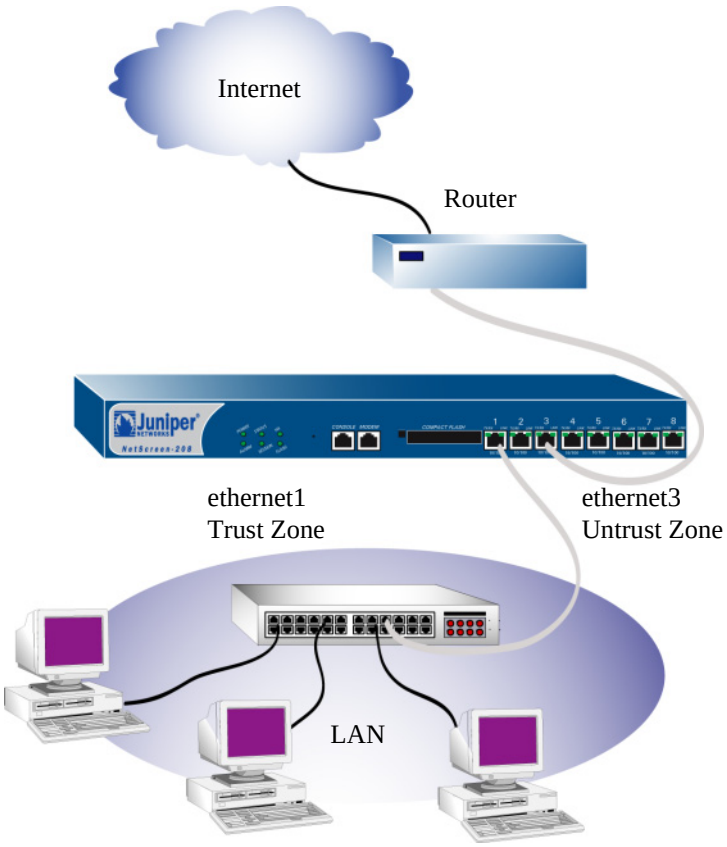
Interface Type	Description
Ethernet interfaces	**ethernet***n* specifies a physical ethernet interface, denoted by a physical port (*n*) on the module. Although each interface is bound to a security zone by default, you can bind it to another zone as required.
	• **ethernet1** Bound to the Trust security zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
	• **ethernet2** Bound to the DMZ security zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
	• **ethernet3** Bound to the Untrust security zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
	• **ethernet4** On NetScreen-204, bound to HA zone by default. On NetScreen-208, bound to the Null zone by default.
	• **ethernet5** through **ethernet7** Bound to Null zone by default.
	• **ethernet8** Bound to the HA zone by default.
Layer-2 interfaces	**vlan1** specifies a logical interface used for management and for VPN traffic termination while the NetScreen device is in Transparent mode.
Tunnel interfaces	**tunnel.***n* specifies a logical tunnel interface. This interface is for VPN traffic.

CONNECTING THE DEVICE AS A SINGLE SECURITY GATEWAY

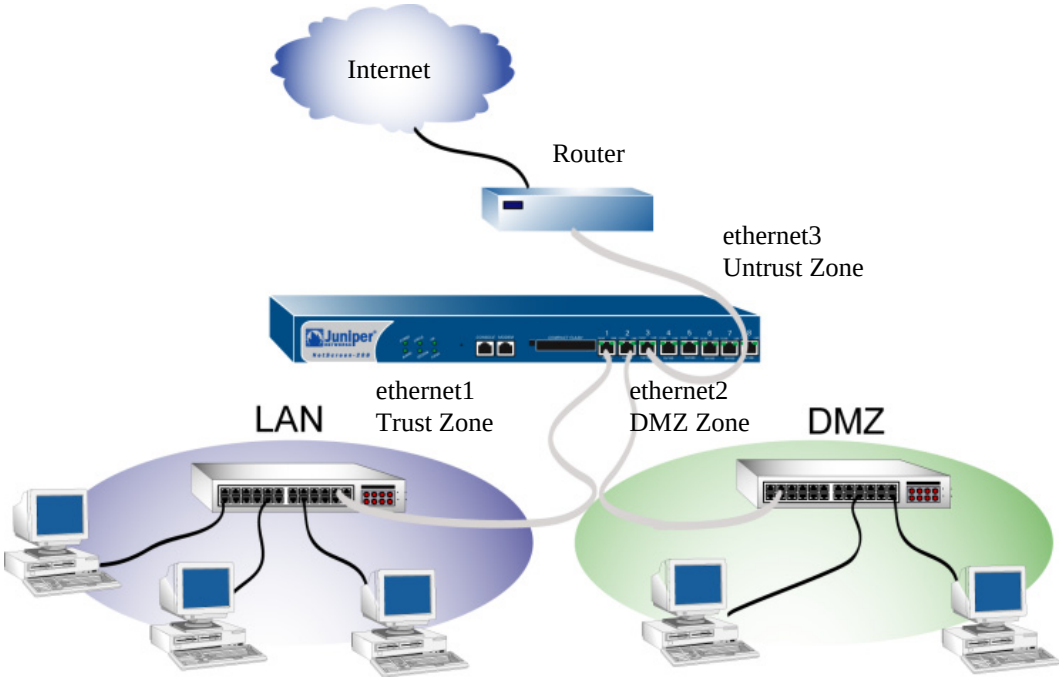
There are many ways to connect a NetScreen-200 Series device to your network system. In most cases, the device serves as a single security gateway that protects at least one LAN (usually connected to the device from a switch or a hub).

Connectivity Examples

In the following example, a NetScreen-208 device connects to the protected LAN through **ethernet1** (bound to the Trust security zone). The device connects externally to a router through **ethernet3** (bound to the Untrust security zone).



In the following example, a NetScreen-208 device connects to a protected LAN through **ethernet1** (bound to the Trust security zone) and to a protected DMZ through **ethernet2** (bound to the DMZ security zone). The device connects externally to a router through **ethernet3** (bound to the Untrust security zone).



Performing Device Connection

The NetScreen-204 device has four ethernet interfaces and the NetScreen-208 has eight. The default **vlan1** IP address and subnet mask of these interfaces is 192.168.1.1/24.

Note: *If you have multiple NetScreen-200 Series devices, install and configure them one at a time. Because they all share the same default* ***vlan1*** *IP address and subnet mask (192.168.1.1/24), you might encounter IP address conflicts.*

To set up the NetScreen-200 Series network connections:

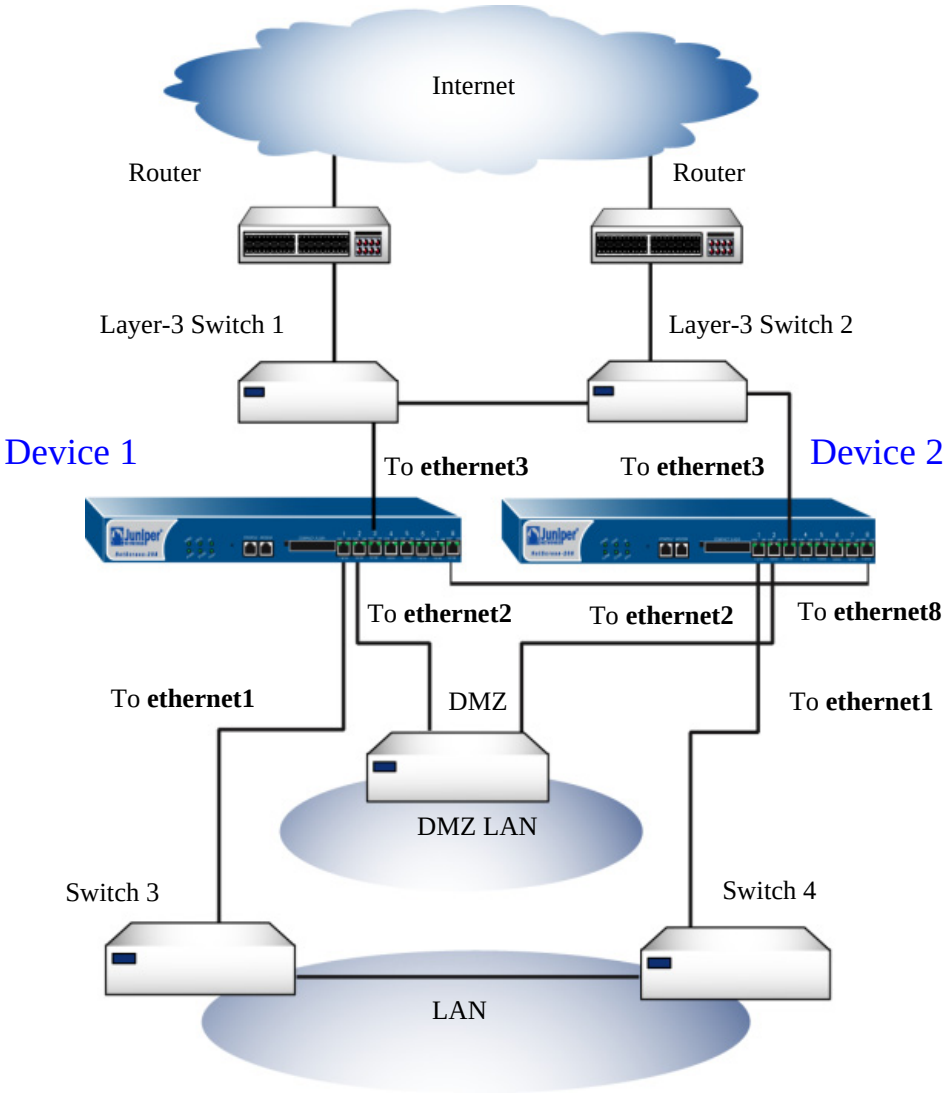
1. Place the NetScreen-200 Series device in a rack or on a desktop.
2. Confirm that the power connection to the device is turned OFF ("**0**" pressed in).
3. Connect the provided power cable from the power outlet to the power supply.
4. Connect the device to the network (see examples above).
5. Turn the NetScreen-200 device power switch ON, then turn the other network device power switches ON. (If all cables are connected correctly, the link light for each connection glows green.)

ESTABLISHING AN HA CONNECTION BETWEEN DEVICES

To assure continuous traffic flow in the event of system failure, you can cable and configure two NetScreen devices in a redundant cluster. The devices propagate all network, configuration and session information to each other. Should one device fail, the other takes over the traffic processing.

Note: *For the NetScreen-204, the default HA interface is* ***ethernet4****. For the NetScreen-208, the default HA interface is* ***ethernet8****. (Each is bound to the HA security zone.)*

The following diagram shows a typical HA setup for NetScreen-208 devices.



Note: *The cabling instructions given below reproduce the configuration shown previously. However, this is not the only possible HA configuration. In addition, the instructions assume that all physical ports and interfaces are set at their default settings. If you have changed the port and interface configurations, the instructions below might not work properly.*

To cable two NetScreen-200 Series devices together for HA and connect them to the network:

1. (Optional) Install the NetScreen-200 Series devices in an equipment rack (see "Equipment Rack Installation Guidelines" on page 10).
2. Make sure that all ON/OFF power supply switches are OFF.
3. Connect the power cables to each NetScreen-200 power supply then connect them to a power source.

   Note: *Whenever you deploy two NetScreen-200 Series devices in an HA cluster, connect each to a different power source, if possible. If one power source fails, the other source might still be operative.*

4. If your device is a NetScreen-204, connect a 10/100 Base-T cable from the **ethernet4** on Device 1 to the **ethernet4** port on Device 2.

   or

   If your device is a NetScreen-208, connect a 10/100 Base-T cable from the **ethernet8** on Device 1 to the **ethernet8** port on Device 2.

Device 1

5. On Device 1, connect a 10/100 Base-T cable from **ethernet1** to the switch labeled "Switch 3."
6. On Device 1, connect a 10/100 Base-T cable from **ethernet2** to the switch labeled "DMZ."
7. On Device 1, connect a 10/100 Base-T cable from **ethernet3** to the switch labeled "Layer 3 switch 1."

Device 2

8. On Device 2, connect a 10/100 Base-T cable from **ethernet1** to the switch labeled "Switch 4."
9. On Device 2, connect a 10/100 Base-T cable from **ethernet2** to the switch labeled "DMZ."
10. On Device 2, connect a 10/100 Base-T cable from **ethernet3** to the switch labeled "Layer 3 switch 2."

Switches

11. Cable together the switches labeled “Switch 3” and “Switch 4.”
12. Cable together the switches labeled “Layer 3 switch 1” and “Layer 3 switch 2.”
13. Cable the switches labeled “Layer 3 switch 1” and “Layer 3 switch 2” to routers.

> ***Note:*** *The switch ports must be defined as 802.1Q trunk ports, and the external routers must be able to use either Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP). For the best configuration method, see the documentation for your switch or router.*

14. Turn the power switches for all devices ON.

For more advanced HA configurations, see the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Performing Initial Connection and Configuration

To establish the first console session with the NetScreen-200 Series device, use a vt100 terminal emulator program through the provided RJ-45/DB9 serial port connector.

Establishing a Terminal Emulator Connection

To establish an initial console session:

1. Plug the DB9 end of the supplied RJ-45/DB-9 serial cable into the serial port of your computer. (Be sure that the DB-9 is seated properly by screwing in the thumbscrews.)
2. Plug the RJ-45 end of the cable into the Console port of the NetScreen-200 Series device. (Be sure that the RJ-45 clip snaps into the port and is seated properly.)
3. Launch a Command Line Interface (CLI) session between your computer and the NetScreen-200 device using a standard serial terminal emulation program such as Hilgraeve Hyperterminal (provided with your Windows operating system). The settings should be as follows:
   - Baud Rate to **9600**
   - Parity to **No**
   - Data Bits to **8**
   - Stop Bit to **1**
   - Flow Control to **none**
4. Press the ENTER key to see the login prompt.
5. At the login prompt, type **`netscreen`**.

6. At the password prompt, type **netscreen**.

   Note: *Use lowercase letters only. Both login and password are case-sensitive.*

7. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To change this timeout interval, execute the following command:

   set console timeout *number*

   where *number* is the length of idle time in minutes before session termination. To prevent any automatic termination, specify a value of **0**.

Changing Your Admin Name and Password

Because all NetScreen products use the admin login name and password (**netscreen**), it is highly advisable to change your admin name and password immediately. Enter the following commands:

```
set admin name name_str
set admin password pswd_str
save
```

For information on creating different levels of administrators, see "Administration" in the *NetScreen Concepts & Examples ScreenOS Reference Guide.*

Setting Port and Interface IP Addresses

Through the CLI, you can execute commands that set IP address and subnet mask values for most of the physical interfaces.

Viewing Current Interface Settings

To begin the configuration process, it is advisable to view existing port settings by executing the following command:

```
get interface
```

This command displays current port names, IP addresses, Zones, MAC addresses, and other useful information.

Setting the IP Address of the Management Interface

To make an interface work as the management interface, you must set the IP address and subnet mask to the same address range as your computer (or LAN). Use the CLI **save** command to save your configuration changes.

To configure the **ethernet1** interface to serve as a management interface:

1. Determine the IP address and subnet mask for your computer (or LAN).
2. Assign the IP address and subnet mask to the **ethernet1** interface by executing the following command:

   set interface ethernet1 ip *ip_addr/mask*

   where *ip_addr* is the IP address and *mask* is the subnet *mask*. For example, to set the IP address and subnet mask of **ethernet1** to 10.100.2.183/16:

   set interface ethernet1 ip 10.100.2.183/16

3. Enable management on the **ethernet1** interface by executing the following command:

   set interface ethernet1 manage

4. (Optional) To confirm the new interface settings, execute the following command:

   get interface ethernet1

Setting the IP Address for the Untrust Zone Interface

The NetScreen-200 Series device usually communicates with external devices through an interface bound to the Untrust zone (such as **ethernet3**). To allow an interface to communicate with external devices, you must assign it a public IP address.

To set the IP address and subnet mask for **ethernet3**:

1. Choose an unused public IP address and subnet mask.
2. Set the **ethernet3** interface to this IP address and subnet mask by executing the following command:

   set interface ethernet3 ip *ip_addr/mask*

   where *ip_addr* is the IP address and *mask* is the subnet mask. For example, to set the IP address and subnet mask of the **ethernet3** interface to 172.16.2.183/16:

   set interface ethernet3 ip 172.16.2.183/16

3. (Optional) To confirm the new port settings, execute the following command:

   get interface ethernet3

Allowing Outbound Traffic

By default, the NetScreen-200 Series device does not allow inbound or outbound traffic, nor does it allow traffic to or from the DMZ. To permit (or deny) traffic, you must create access policies.

The following CLI command creates an access policy that permits all kinds of outbound traffic, from any host in your trusted LAN to any device on the untrusted network.

```
set policy from trust to untrust any any any permit
```

Save you access policy configuration with the following command:

```
save
```

Note: *Your network might require a more restrictive policy than the one created in the example above. The example is NOT a requirement for initial configuration. For detailed information about access policies, see the NetScreen Concepts & Examples ScreenOS Reference Guide.*

You can also use the Outgoing Policy Wizard in the WebUI management application to create access policies for outbound traffic. See "Establishing a GUI Management Session" on page 26 for information on accessing the WebUI application.

Configuring the Device for Telnet and WebUI Sessions

In addition to terminal emulator programs, you can use Telnet (or dialup) to establish console sessions with the NetScreen-200 Series device. In addition, you can start management sessions using the NetScreen WebUI, a web-based GUI management application.

Starting a Console Session Using Telnet

To establish a Telnet session with the NetScreen-200 Series device:

1. Connect an RJ-45 cable from **ethernet1** to the internal switch, router, or hub in your LAN (see "Connecting the Device as a Single Security Gateway" on page 18).
2. Open a Telnet session, specifying the current IP address for **ethernet1**. For example, in Windows, click **Start >> Run**, enter **telnet** *ip_addr* (where *ip_addr* is the address of the **ethernet1** interface), then click **OK**.

   For example, if the current address of the **ethernet1** interface is 10.100.2.183, enter:

   telnet 10.100.2.183
3. At the Username prompt, type your user name (default is **netscreen**).
4. At the Password prompt, type your password (default is **netscreen**).

   Note: *Use lowercase letters only. Both username and password are case-sensitive.*

5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To change this timeout interval, execute the following command:

   set console timeout *number*

   where *number* is the length of idle time in minutes before session termination. To prevent any automatic termination, specify a value of **0**.

Starting a Console Session Using Dialup

Each NetScreen-200 Series device provides a modem port that allows you to establish a remote console session using a dialup connection through a 9600 bps modem cabled to the modem port. Dialing into the modem establishes a dialup console connection.

Note: *The Terminal type for dialup sessions must be vt100. For example, in Hilgreave HyperTerminal (a commonly-used terminal application), select* ***Connect >> Remote System****, then select* ***vt100*** *from the Term Type menu.*

Establishing a GUI Management Session

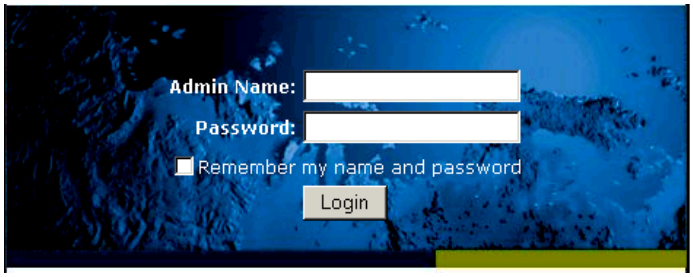
To access the NetScreen-200 Series device with the WebUI management application:

1. Connect your computer (or your LAN hub) to the **ethernet1** port using a Category-5 Ethernet cable.
2. Launch your browser, enter the IP address of the **ethernet1** interface in the URL field, and then press Enter.

   For example, if you assigned the **ethernet1** interface an IP address of 10.100.2.183/16, enter the following:

   `10.100.2.183`

   The NetScreen WebUI software displays the login prompt.



3. Enter **netscreen** in both the **Admin Name** and **Password** fields, then click **Login**. (Use lowercase letters only. The Admin Name and Password fields are both case sensitive.)

The NetScreen WebUI application window appears.

Note: *NetScreen-Security Manager 2004 (NSM) and NetScreen Rapid Deployment (RD): If you are using NSM, you can optionally configure NetScreen appliances with RD. Refer to the* Rapid Deployment Getting Started Guide *for more information.*

ASSET RECOVERY

If you lose the admin password, you can use one of the following procedures to reset the NetScreen device to its default settings. This destroys any existing configurations, but restores access to the device.

Warning: *Resetting the device will delete all existing configuration settings, and the firewall and VPN service will be rendered inoperative.*

Note: *After you successfully reset and reconfigure the NetScreen device, you should back up the new configuration setting. As a precaution against lost passwords, you should back up a new configuration that contains the NetScreen default password. This will ensure a quick recovery of a lost configuration. You should change the password on the system as soon as possible.*

Using CLI Commands to Reset the Device

To perform this operation, you need to make a console connection, as described in "Establishing a Terminal Emulator Connection" on page 22.

Note: *By default the device recovery feature is enabled. You can disable it by entering the following CLI command:* ***unset admin device-reset****.*

1. At the login prompt, type the serial number of the device.
2. At the password prompt, type the serial number again.

   The following message appears:

   !!! Lost Password Reset !!! You have initiated a command to reset the device to factory defaults, clearing all current configuration and settings. Would you like to continue? y/[n]

3. Press the **y** key.

   The following message appears:

   !! Reconfirm Lost Password Reset !! If you continue, the entire configuration of the device will be erased. In addition, a permanent counter will be incremented to signify that this device has been reset. This is your last chance to cancel this command. If you proceed, the device will return to factory default configuration, which is: System IP: 192.168.1.1; username: netscreen; password: netscreen. Would you like to continue? y/[n]

4. Press the **y** key to reset the device.

   You can now login in using *netscreen* as the default admin name and password.

Using the Asset Recovery Pinhole to Reset the Device

You can also reset the device and restore the factory default settings by pressing the asset recovery pinhole. To perform this operation, you need to make a console connection, as described in "Establishing a Terminal Emulator Connection" on page 22.

1. Locate the asset recovery pinhole on the front panel (see "The Front Panel" on page 3). Using a thin, firm wire (such as a paper clip), push the button located behind the asset recovery pinhole for four to six seconds.

   A serial console message states that the "Configuration Erasure Process has been initiated" and the system sends an SNMP/SYSLOG alert. The Status LED blinks amber once every second.

   After the first reset is accepted, the power LED blinks green. The serial console message now reads, "Waiting for 2nd confirmation."

2. Release the button for one second.
3. Push the button again for four to six seconds. A serial console message states "Second push has been confirmed."

   The Status LED lights amber for one-half second, then returns to the blinking green state. Continue to press the button until the message "Configuration Erase sequence accepted, unit reset." The system generates SNMP and SYSLOG alerts to configured SYSLOG or SNMP trap hosts.

   Note: *During a reset, there is no guarantee that the final SNMP alert sent to the receiver before the reset will be received.*

4. Release the button.
5. The device now erases the configuration and restarts.

If you do not follow the complete sequence, the reset process cancels without any configuration change and the serial console message states, "Configuration Erasure Process aborted." The status LED returns to blinking green. If the unit did not reset, an SNMP alert is sent to confirm the failure.

Specifications

A

This appendix provides general system specifications for the NetScreen-200 Series devices.

NetScreen-200 Attributes

Height:1.73 inches (4.4 cm)

Depth:10.8 inches (27.4 cm)

Width:17.5 inches (44.5 cm)

Weight: 8 pounds (36 hg)

Electrical Specification

AC voltage:100-240 VAC +/- 10%

DC voltage:-36 to -60 VDC

AC Watts:45 Watts

DC Watts:50 Watts

Fuse Rating:2.5Amps / 250Volts

Environmental

Temperature	Operating	Non-operating
Normal altitude	0°-50° C, 32-122° F	-40°-158° F, -40°-70° C
Relative humidity	10-90%	5-95%
Non-condensing	10-90%	5-95%

The maximum normal altitude is 0 - 12,000 ft. (0 - 3,660 m)

NEBS Certifications

Level 3 (NetScreen-208 with DC power)

GR-63-Core: NEBS, Environmental Testing

GR-1089-Core: EMC and Electrical Safety for Network Telecommunications Equipment

Safety Certifications

UL, CUL, CSA, CB, Austel, CE

EMI Certifications

FCC class A, BSMI, CE class A, C-Tick, VCCI class A

Index

S

T

V